

**CLAIMS:**

What is claimed is:

1. A method of operating an electronic locking device  
5 using a wireless communication device, comprising:  
receiving a master key code from a master key  
supplier;  
generating a secondary key code from the master key  
code; and  
transmitting the secondary key code to the wireless  
communication device, wherein the secondary key code is  
used by the wireless communication device to operate the  
electronic locking device.
- 15 2. The method of claim 1, wherein the secondary key  
code includes a secondary key code portion and zero or  
more of a master key code portion, an activation/  
expiration portion, a wireless communication device  
identification portion, a time of issue portion, and a  
20 time of last use portion.
3. The method of claim 1, wherein the master key code  
is received via at least one network.
- 25 4. The method of claim 1, further comprising:  
sending a master key code request to the master key  
supplier, the master key code request identifying one or  
more of a key supplier identifier, a product code of the  
electronic locking device, an electronic certificate, and  
30 a password.
5. The method of claim 1, further comprising:  
transmitting the secondary key code to the

Sub  
10  
15  
20  
25  
30  
35  
40  
45  
50  
55  
60  
65  
70  
75  
80  
85  
90  
95  
100  
105  
110  
115  
120  
125  
130  
135  
140  
145  
150  
155  
160  
165  
170  
175  
180  
185  
190  
195  
200  
205  
210  
215  
220  
225  
230  
235  
240  
245  
250  
255  
260  
265  
270  
275  
280  
285  
290  
295  
300  
305  
310  
315  
320  
325  
330  
335  
340  
345  
350  
355  
360  
365  
370  
375  
380  
385  
390  
395  
400  
405  
410  
415  
420  
425  
430  
435  
440  
445  
450  
455  
460  
465  
470  
475  
480  
485  
490  
495  
500  
505  
510  
515  
520  
525  
530  
535  
540  
545  
550  
555  
560  
565  
570  
575  
580  
585  
590  
595  
600  
605  
610  
615  
620  
625  
630  
635  
640  
645  
650  
655  
660  
665  
670  
675  
680  
685  
690  
695  
700  
705  
710  
715  
720  
725  
730  
735  
740  
745  
750  
755  
760  
765  
770  
775  
780  
785  
790  
795  
800  
805  
810  
815  
820  
825  
830  
835  
840  
845  
850  
855  
860  
865  
870  
875  
880  
885  
890  
895  
900  
905  
910  
915  
920  
925  
930  
935  
940  
945  
950  
955  
960  
965  
970  
975  
980  
985  
990  
995

Docket No. AUS9-2000-0560-US1

electronic locking device using at least one of a wired communication link and wireless communication link.

5 6. The method of claim 5, wherein transmitting the secondary key code to the electronic locking device includes transmitting the secondary key code based on a network address of the electronic locking device.

10 7. The method of claim 5, wherein transmitting the secondary key code to the electronic locking device includes broadcasting the secondary key code along with an identifier of the electronic locking device.

15 8. The method of claim 1, wherein the wireless communication device is one of a personal digital assistant, a two-way pager, a mobile telephone device, a wireless transmitter, a handheld computer, a laptop computer, and a Bluetooth™ enabled device.

20 9. The method of claim 1, wherein transmitting the secondary key code to the wireless communication device includes transmitting the secondary key code using at least one of a wireless communication link and a wired communication link.

25 10. The method of claim 1, wherein transmitting the secondary key code to the wireless communication device includes transmitting the secondary key code as an attachment to an electronic mail message.

30 11. The method of claim 10, wherein the electronic mail message is sent to the wireless communication device at a remote time from use of the secondary key code to operate

007271-1254250

the electronic locking device.

12. The method of claim 5, further comprising receiving  
a confirmation message from the electronic locking device  
5 confirming reprogramming of the electronic locking device  
to accept the secondary key code.

13. The method of claim 1, wherein the electronic  
locking device is preprogrammed to accept the secondary  
10 key code.

14. The method of claim 5, wherein transmitting the  
secondary key code to the electronic locking device is  
performed at a remote time from transmitting the  
15 secondary key code to the wireless communication device.

15. The method of claim 1, further comprising:  
receiving a key code from the wireless communication  
device;  
20 authenticating the key code based on the secondary  
key code; and  
transmitting a command to operate the electronic  
locking device if the key code is authentic.

25 16. The method of claim 15, further comprising:  
determining if a number of attempts to operate the  
electronic locking device within a predetermined period  
of time exceeds a threshold; and  
placing the electronic locking device in a safety  
30 mode if the number of attempts exceeds the threshold.

17. The method of claim 16, wherein the safety mode is  
one of a slow down mode and a freeze mode.

09717521.112100

5

10

15

20

25

30

24. The method of claim 15, wherein authenticating the key code based on the secondary key code includes determining an activation/expiration time of the secondary key code and determining if a current time is within the activation/expiration time.
25. The method of claim 3, wherein the at least one network is the Internet.
26. The method of claim 1, further comprising:  
polling the electronic locking device; and  
receiving status information from the electronic locking device in response to polling the electronic locking device.
27. The method of claim 26, wherein the status information includes at least one of a current status of the electronic locking device, a time at which operation of the electronic locking device was last attempted, a key code last used to attempt to operate the electronic locking device, and a wireless communication device identifier of a wireless communication device last used to attempt to operate the electronic locking device.
28. The method of claim 26, further comprising operating the electronic locking device based on the received status information.
29. An apparatus for operating an electronic locking device using a wireless communication device, comprising:  
means for receiving a master key code from a master key supplier;

09747521-112400

means for generating a secondary key code from the master key code; and

first means for transmitting the secondary key code to the wireless communication device, wherein the  
5 secondary key code is used by the wireless communication device to operate the electronic locking device.

30. The apparatus of claim 29, wherein the secondary key code includes a secondary key code portion and zero or  
10 more of a master key code portion, an activation/expiration portion, a wireless communication device identification portion, a time of issue portion, and a time of last use portion.

31. The apparatus of claim 29, wherein the master key code is received from the master key supplier via at  
15 least one network .

32. The apparatus of claim 29, further comprising:  
20 means for sending a master key code request to the master key supplier, the master key code request identifying one or more of a key supplier identifier, a product code of the electronic locking device, an electronic certificate, and a password.

33. The apparatus of claim 29, further comprising:  
25 second means for transmitting the secondary key code to the electronic locking device using at least one of a wired communication link and wireless communication link.

34. The apparatus of claim 33, wherein the second means for transmitting the secondary key code to the electronic  
30 locking device includes means for transmitting the

00717531-112100

secondary key code based on a network address of the electronic locking device.

35. The apparatus of claim 33, wherein the second means  
5 for transmitting the secondary key code to the electronic locking device includes means for broadcasting the secondary key code along with an identifier of the electronic locking device.

10 36. The apparatus of claim 29, wherein the wireless communication device is one of a personal digital assistant, a two-way pager, a mobile telephone device, a wireless transmitter, a handheld computer, a laptop computer, and a Bluetooth™ enabled device.

15 37. The apparatus of claim 29, wherein the first means for transmitting the secondary key code to the wireless communication device includes means for transmitting the secondary key code using at least one of a wireless  
20 communication link and a wired communication link.

38. The apparatus of claim 29, wherein the first means for transmitting the secondary key code to the wireless communication device includes means for transmitting the  
25 secondary key code as an attachment to an electronic mail message.

39. The apparatus of claim 38, wherein the electronic mail message is sent to the wireless communication device  
30 at a remote time from use of the secondary key code to operate the electronic locking device.

40. The apparatus of claim 33, further comprising means

09717531.112100

Docket No. AUS9-2000-0560-US1

for receiving a confirmation message from the electronic locking device confirming reprogramming of the electronic locking device to accept the secondary key code.

5 41. The apparatus of claim 29, wherein the electronic locking device is preprogrammed to accept the secondary key code.

42. The apparatus of claim 33, wherein the second means  
10 for transmitting the secondary key code to the electronic  
locking device performs the transmission at a remote time  
from transmitting the secondary key code to the wireless  
communication device.

43. The apparatus of claim 29, further comprising:  
means for receiving a key code from the wireless  
communication device;  
means for authenticating the key code based on the  
secondary key code; and  
means for transmitting a command to operate the  
electronic locking device if the key code is authentic.

44. The apparatus of claim 43, further comprising:  
means for determining if a number of attempts to  
25 operate the electronic locking device within a  
predetermined period of time exceeds a threshold; and  
means for placing the electronic locking device in a  
safety mode if the number of attempts exceeds the  
threshold.

30

45. The apparatus of claim 44, wherein the safety mode is one of a slow down mode and a freeze mode.



46. The apparatus of claim 43, wherein the means for authenticating the key code includes means for performing a comparison of the key code to information stored in a key code table.

47. The apparatus of claim 46, wherein the key code table includes an entry for the electronic locking device, and wherein the entry includes one or more of a valid secondary key code, activation/expiration information, and wireless communication device identification information.

10

15

20

25

30

52. The apparatus of claim 43, wherein the means for authenticating the key code based on the secondary key code includes determining an activation/expiration time of the secondary key code and determining if a current  
5 time is within the activation/expiration time.

53. The apparatus of claim 31, wherein the at least one network is the Internet.

10 54. The apparatus of claim 29, further comprising:  
means for polling the electronic locking device; and  
means for receiving status information from the electronic locking device in response to polling the electronic locking device.

15 55. The apparatus of claim 54, wherein the status information includes at least one of a current status of the electronic locking device, a time at which operation of the electronic locking device was last attempted, a  
20 key code last used to attempt to operate the electronic locking device, and a wireless communication device identifier of a wireless communication device last used to attempt to operate the electronic locking device.

25 56. A computer program product in a computer readable medium for operating an electronic locking device using a wireless communication device, comprising:

first instructions for receiving a master key code from a master key supplier;

30 second instructions for generating a secondary key code from the master key code; and

third instructions for transmitting the secondary key code to the wireless communication device, wherein

007251.1100

Docket No. AUSS-2000-0560-US1

the secondary key code is used by the wireless communication device to operate the electronic locking device.

- 5 57. A method of operating an electronic locking device using a wireless communication device, comprising:
- requesting a secondary key code from a key code supplier;
  - receiving the secondary key code associated with the
  - 10 electronic locking device, the secondary key code having been generated based on a master key code; and
  - transmitting the secondary key code to the
  - electronic locking device, wherein the electronic locking device is operated in response to receiving the secondary
  - 15 key code.

58. The method of claim 57, wherein the secondary key code includes a secondary key code portion and zero or more of a master key code portion, an activation/
- 20 expiration portion, a wireless communication device identification portion, a time of issue portion, and a time of last use portion.

59. The method of claim 57, wherein the wireless
- 25 communication device is one of a personal digital assistant, a two-way pager, a mobile telephone device, a wireless transmitter, a handheld computer, a laptop computer, and a Bluetooth™ enabled device.

- 30 60. The method of claim 57, wherein receiving the secondary key code includes receiving the secondary key code as an attachment to an electronic mail message.

0071251.12100

Docket No. AUS9-2000-0560-US1

61. The method of claim 60, wherein the electronic mail message is received at a remote time from use of the secondary key code to operate the electronic locking device.

5

62. The method of claim 57, wherein the electronic locking device is preprogrammed to accept the secondary key code.

10

63. The method of claim 58, wherein the secondary key code portion and the one or more of a master key code portion, an activation/expiration portion, a wireless communication device identification portion, a time of issue portion, and a time of last use portion are encoded.

15

64. The method of claim 57, further comprising:  
determining if a delete command is received; and  
deleting the secondary key code from a key storage  
if a delete command is received.

20

65. The method of claim 64, wherein the delete command is received from one of a key supplier and the electronic locking device.

25

66. A wireless communication apparatus for operating an electronic locking device, comprising:

means for requesting a secondary key code from a key code supplier;

30

means for receiving the secondary key code associated with the electronic locking device, the secondary key code having been generated based on a master key code; and

0071521-113100

means for transmitting the secondary key code to the electronic locking device, wherein the electronic locking device is operated in response to receiving the secondary key code.

5

67. The wireless communication apparatus of claim 66, wherein the secondary key code includes a secondary key code portion and zero or more of a master key code portion, an activation/expiration portion, a wireless communication device identification portion, a time of issue portion, and a time of last use portion.

10

68. The wireless communication apparatus of claim 66, wherein the wireless communication apparatus is one of a personal digital assistant, a two-way pager, a mobile telephone device, a wireless transmitter, a handheld computer, a laptop computer, and a Bluetooth™ enabled device.

15

69. The wireless communication apparatus of claim 66, wherein the means for receiving the secondary key code includes means for receiving the secondary key code as an attachment to an electronic mail message.

20

70. The wireless communication apparatus of claim 69, wherein the electronic mail message is received at a remote time from use of the secondary key code to operate the electronic locking device.

25

71. The wireless communication apparatus of claim 66, wherein the electronic locking device is preprogrammed to accept the secondary key code.

30

09717521.112100

Docket No. AUSS-2000-0560-US1

72. The wireless communication apparatus of claim 67,  
wherein the secondary key code portion and the zero or  
more of a master key code portion, an activation/  
expiration portion, a wireless communication device  
5 identification portion, a time of issue portion, and a  
time of last use portion are encoded.

73. The wireless communication apparatus of claim 66,  
further comprising:  
10 means for determining if a delete command is  
received; and  
means for deleting the secondary key code from a key  
storage if a delete command is received.

74. The wireless communication apparatus of claim 73,  
wherein the delete command is received from one of a key  
supplier and the electronic locking device.

75. A computer program product in a computer readable  
20 medium for operating an electronic locking device,  
comprising:

first instructions for requesting a secondary key  
code from a key code supplier;  
second instructions for receiving the secondary key  
25 code associated with the electronic locking device, the  
secondary key code having been generated based on a  
master key code; and

third instructions for transmitting the secondary  
key code to the electronic locking device, wherein the  
30 electronic locking device is operated in response to  
receiving the secondary key code.

76. A method of operating an electronic locking device

09747524.112100

Docket No. AUS9-2000-0560-US1

using a wireless communication device, comprising:

receiving, from a key supplier, a secondary key code for operating the electronic locking device, the secondary key code having been generated based on a master key code;

receiving a key code from the wireless communication device;

authenticating the key code using the secondary key code; and

operating the electronic locking device if the key code is authenticated.

77. An electronic locking device comprising:

means for receiving, from a key supplier, a secondary key code for operating the electronic locking device, the secondary key code having been generated based on a master key code;

means for receiving a key code from a wireless communication device;

means for authenticating the key code using the secondary key code; and

means for operating the electronic locking device if the key code is authenticated.

78. A computer program product in a computer readable medium for operating an electronic locking device, comprising:

first instructions for receiving, from a key supplier, a secondary key code for operating the electronic locking device, the secondary key code having been generated based on a master key code;

second instructions for receiving a key code from the wireless communication device;

09717521-112100

Docket No. AUS9-2000-0560-US1

~~third instructions for authenticating the key code  
using the secondary key code; and~~

~~fourth instructions for operating the electronic  
locking device if the key code is authenticated.~~

09717521.112100